者など特定の役職員が個人データにアクセスできないよう、パスワードを設けるなどの措置や、故意又は過失による虚偽入力、書き換え及び消去ができないようにシステムを構築するなど、十分なセキュリティ対策を講ずる。

① パソコン等の機器によって個人情報を処理する場合は、担当者もしくは担当課長、係長などしかアクセスできないように、ＩＤ及びパスワードを入力しなければ作動しないようにシステムを構築する。

② 作業室が設置されている場合は、入室についても、特定の鍵などを保有しない人が出入りできないようにする。

③ ＩＤパスワードの管理は、担当者個人に管理責任を負わせるとともに、他人が容易に分かる場所等にＩＤパスワードを記載したり、他人に教えたりしないように周知徹底する。

④ 業務処理用のパソコン等は、リスクを少なくするためにできるだけ専用の端末とし、インターネットを行うパソコン等とは明確に区別すべきである。

⑤ 業務用パソコンをインターネット（メールを含む）に接続する場合は、最新のセキュリティ対策に努め、各パソコンには最新のウイルスチェックソフトの投入、ファイヤウォールを設けるなど、外部からの侵入に対する対策を講ずる。

⑥ ペーパーによる個人情報の管理の場合も、同様に盗難、紛失、不正利用等がないよう施錠をするなど十分な措置を講ずる。

【パソコン等の処分】

① パソコンやサーバ等の廃棄又は転売・譲渡等（リースの場合は返却）を行う場合は、最新のハードディスクデータ消去ツール等を使用するか、又はデータ消去を専門に取り扱う業者に委託するなど、内部のデータが復元されないような措置を講ずる。この場合の業者委託については、データの消去に立ち会い、又は復元テストを行うなど、確実に消去されたことを確認する。

② ハードディスクを物理的に破壊する方法が最も確実であるが、破壊の際は環境問題等にも十分に考慮した上で措置を講ずる必要がある。なお、この場合においても、破壊する現場に立ち会い、又は手渡したハードディスクを確実に破壊した証拠写真やビデオ等の提出を求め、確認する。

③ 個人情報の記載されたペーパーを廃棄する場合は、シュレッダーにかけて読み取り不能にする。

④ 大量の個人情報記載用紙等を廃棄する場合は、信頼できる専門の溶解・破砕業者に処理を委託する。この場合は、溶解・破砕の処理工程を見学し、管理体制の整っている業者であるかどうかを確認する必要がある。また、破砕車による現地破砕業者に委託し、破砕時には立ち会いなどを行う。ただし、その実施依頼は、環境問題等を考慮し焼却業者はできるだけ避けるものとする。

苦情処理・顧客への対応

個人情報保護法31条では、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努め、そのために必要な体制を整備することを定めている。

健診機関としては、顧客側から個人情報の保護についての要請や指導を受けても委託契約の条項となりうる上記の対策とともに苦情への対応を講ずる必要がある。

【対　策】

① 苦情を受ける部署及び担当者を設定する。
② 苦情処理に対する内部手続きを定めて周知徹底する。
③ 苦情処理担当者は、定期的に研修などを行い必要な知識を身につける。
④ 広域的に事業を展開している場合は、各活動拠点での窓口設定や複数の通信手段の対応の整備も必要である。
⑤ 個人情報に係る事故が発生した場合は、速やかに顧客に報告する。

【顧客への対応】

① 個人情報の保護については、顧客側からの要請や指導についても委託契約の条項となるようにする。
② 個人情報に係る事故が発生した場合は、速やかに顧客へ報告する。

業務の再委託について

受託した健診事業の業務を外部に再委託する場合は、その外部業者に対しても個人情報保護に関する理解と遵守について、周知徹底をはかり正確性・安全性を確保することが義務づけられる。以下、受託事業の再委託時における個人情報保護に関する対応を述べる。

【再委託の定義】

再委託とは次の業務を外部業者に外注することをいう。

①検診業務：　エックス線撮影等の画像診断や心電図等の外部機関の医師への判定依頼など。
②検査依頼：　血液等の検体処理依頼。
③電子計算機システムのオペレーション：　データ入力業務や報告書等作成などの情報処理業務。
④電子計算機システムの構築や管理：　社内システム、電子計算機器、データベースの構築や保守、点検、管理の外注。
⑤電子計算機システムのＡＳＰ業務：　インターネット利用やデータベース等の外部管理。
⑥ソフトウエア制作：　大規模システムから小規模アプリケーション等のソフトウ

エア制作の外注。

⑦媒体の保管：　個人情報を保存したＦＤ、ＭＯ等の記録媒体を外部業者に保管管理委託。

⑧その他：　建物内の警備や清掃業務などの外注。

【目的等の明確化】

業務を再委託する場合は、目的と方針を明確にする。

①自機関の設備、能力、技術等の不備による場合。

②コストダウンを図るため外部委託が有利の場合。

③納期確保に有利な場合。

④その他。

【外部業者の選定】

①外部業者の選定にあたっては、プライバシーマーク認証取得業者、ＩＳＯ9000認証取得業者、医療評価認証取得機関又は十分な個人情報の保護水準を満たしている業者を選定する。また、既に委託している業者においても、改めて個人情報保護について十分な管理能力があるか否かを再調査し委託継続の検討をはかる。

②外部業者の選定にあたっては、経営・技術能力、業務実績、主な取引状況などを十分に調査して選定する。

③外部業者の決定に当たっては、業務担当の幹部職が業務委託の必要性と妥当性について部門長と十分に協議・検討し、個人情報保護部門管理者の承認を得て行うものとする。

【契約の締結】

外部業者に業務を再委託する場合は、以下の項目を明記した「基本（委託）契約書」を締結することを了承した業者に委託する。

なお、基本（委託）契約書とは別に以下の項目が盛り込まれた「個人情報の保護に関する契約書」（仮称）を別途に作成して契約する方法もある。

①個人情報の守秘義務に関する事項

業務上知り得た個人情報は正当な理由なく他に開示、提供又は漏洩してはならない。また、業務の遂行以外のいかなる目的にも使用してはならない。

②個人情報の管理義務に関する事項

個人情報に関わる処理方法を遵守し十分な配慮を持ってこれを管理する。個人情報への不当なアクセス又は紛失、破壊、改ざん及び漏洩などの危険に対して、技術面及び組織面において合理的な安全対策を講じる。

③個人情報の開示・訂正・削除に関する事項

本人から情報開示の請求があった場合には、受診者はすみやかに受託者あて連絡をするものとし、委託者において処理するものとする。個人情報に誤りがあって、本人より訂正又は削除の請求を受けた時も同様とする。

④目的範囲外の個人情報収集、利用及び提供の禁止事項

委託した業務を遂行するために預託した個人情報について、それ以外の目的に

利用してはならない。

⑤個人情報の受渡しについての取決めに関する事項

個人情報の授受、運搬は、書面によりその記録を残さなければならない。

⑥保管場所、保管方法についての取決めに関する事項

個人情報を保管庫による施錠管理又はコンピュータ等におけるパスワード設定、個人情報の暗号化等を行い、正当な権限を有したアクセス者以外の者が参照、入力、出力、複製、編集等の利用ができないよう適正に管理しなければならない。

⑦個人情報の廃棄及び消去に関する事項

委託された個人情報を業務目的が終了したときは、速やかに責任を持って返却もしくは廃棄をしなければならない。

⑧再委託の禁止事項

委託された業務を再委託してはならない。

⑨個人情報保護に係る管理状況の監査権限

あらかじめ通知の上、事務所に立ち入り個人情報の管理状況を監査する事ができるものとする。監査の結果又はその他により契約に違反していると判断した場合には、個人情報の使用の差し止め請求ができるものとする。その際は、個人情報及び個人情報により作成した全てのものを返還又は引き渡さなければならない。個人情報の管理方法について改善を申し入れた場合には、これに従わなければならない。

⑩その他、委託業務の種類に応じた必要な事項

⑪前項の定めに違反した場合における損害賠償に関する事項

個人情報への不当なアクセス又は紛失、破壊、改ざん若しくは漏洩等の事故が発生した際、その事故が業者の責に帰すべきものである場合において、情報主体から損害賠償請求その他の請求を受けたときは、その解決のために要した費用（損害賠償金、和解金、弁護士費用等）を賠償する責を負うものとする。

(5) 個人情報保護に関する遵守の周知徹底

業務を外部業者に再委託する際には、契約事項を遵守し履行させることが原則となるが、個人情報保護に関する遵守については、以下に定める重要事項に関し再度周知徹底をはかる。

①個人情報保護に関する法令及びその他の規範を遵守すること。

②個人情報保護に関する適切な教育が行われていなければならない。

研修の頻度や方法等を内部規程で定め、それを遵守するものとする。

③本人から個人情報の開示を求められた場合に備え、窓口の設置と対応措置。

苦情相談も兼ねた窓口と担当者を任命しておく必要がある。担当者不在のときの対応もあらかじめ策定しておく必要がある。

④再委託する目的範囲外の個人情報収集、利用及び第三者への提供を禁止する。

目的範囲外の個人情報の収集、利用及び提供を行う場合は、明確にその旨を本人

に伝え必ず同意を得ること。なお、次のいずれかに該当する場合は、本人の同意を必要としない。

a.法令の規定による場合。

b.本人又は公衆の生命、健康、財産などの重大な利益を保護するために必要な場合。

⑤個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩のリスクを認識させ、次の事項について予防と是正に務める。

a.建物や部屋の強度や入退出の制限、施錠などの物理的セキュリティ対策。

b.個人情報へのアクセス権限や制限措置を講ずる組織的セキュリティ対策。

c.インターネット／アクセス制限を講ずるネットワークセキュリティ対策。

d.ウィルスの混入防止の措置を講ずるコンピュータセキュリティ対策。

健康診断機関における個人情報の保護に関するガイドライン

平成16年3月15日　発行

定価 1,000円（税込み）

編　　集　社団法人 全国労働衛生団体連合会

発 行 所　社団法人 全国労働衛生団体連合会

発 行 人　梶川　清

〒108－0014　東京都港区芝４－４－５
三田労働基準協会ビル４階
TEL 03－5442－5934
FAX 03－5442－5937